

News & Update

- SVRP
- AiSP Cyber Wellness
- Special Interest Groups
- The Cybersecurity Awards
- Regionalisation
- Digital For Life
- Upcoming Events

Contributed Contents

- CISO SIG: Introducing CISO with a deep interest in cybersecurity
- AI SIG: Artificial Intelligence 101
- AiSP Cloud Security Summit Sponsor: Tenable Named a CRN 2024 Cloud 100 Company
Tenable continues to innovate and advance its market-leading cloud security solution
- AiSP Cloud Security Summit Sponsor: The Blueprint for Securing the Hybrid Cloud: Essential Cloud Security Training
- SVRP 2023 Gold Winner, Elton Tay Chee Hean

Professional Development Membership

NEWS & UPDATE

New Partners

AiSP would like to welcome HTX and Proofpoint as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

New Corporate Partner



proofpoint®

News & Updates

Anti-Scam Awareness Workshop by Grab on 2-3 September

AiSP was invited to the Anti-Scam Awareness Workshop at our CPP Grab office to share with the Grab Drivers & Delivery Personnel to beware of scam on 2 – 3 September. Thank you Ms Rahayu Mahzam for gracing the event and Ms Catherine Lee and Grab for inviting AiSP and Ms Wendy Ng for the sharing!



Member Acknowledgment

Interview with AiSP EXCO Member Mr Stanley Eu



1. What is your vision for your contribution in AiSP? What do you think is the biggest issue in the Cybersecurity Industry?

Firstly, thank you for the opportunity to give a background and outlook of myself. My vision is to build a community of like-minded practitioners and students who are passionate about security in the development stage and add their collective knowledge and practices to AiSP. Many cybersecurity issues are manifested at the late stage and most of us are trying to play catch up. If we can 'Shift Left, but Keep Right' in our test phase, we can test out bugs early before it's too big a problem!

2. As the Exco member, there are times where you will be representing AiSP in events and engagements. How do you plan to uphold AiSP's reputation and values while effectively communicating its mission and objectives to external stakeholders?

Honestly, as part of the Cybersecurity industry, every member (not just the Exco) should uphold the integrity and values of AiSP such as being professional and to cooperate & collaborate with one another. Exco members are just standing more in the forefront at events and engagements. So, a strong & clear message should be developed to consistently shared with members and stakeholders and to update it by listening and engaging with members during events and networking sessions.

3. Lastly, what would you like to share and contribute your expertise with our AiSP members and the wider community?

Well, I've been working in the IT industry for more than 30 years and I believe that 'Vision without Execution, is Hallucination!' And Security and Stability ensures the Quality of the applications and systems. Thus, my hope is that organisations would put investments into their vision to build a secure environment and quality applications, starting from development (outsourced or in-house) all the way to monitoring their end points. In the end, I've learnt that successful deployments are based on 4Ps: Policy, Process, Products, People. I wish everyone all the best in their Cybersecurity journey.

Student Volunteer Recognition Programme (SVRP)

Learning Journey to Brunei from 17 September to 20 September

As part of the 40th anniversary of diplomatic relation between Singapore & Brunei, AiSP brought students on an overseas learning journey to Brunei from 17 - 20 September supported by the National Youth Council.



Learning Journey to Brunei Day 1, 17 September

The students visited Cyber Security Brunei for the first visit in Brunei on 17 September. Thank you Brunei Cyber Security Association for coordinating and Cyber Security Brunei for hosting.



Learning Journey to Brunei Day 2, 18 September

On 18 September, the students visited Unified National Networks (UNN). Thank you Brunei Cyber Security Association for coordinating and UNN for hosting.



The students also visited EVYD Technology as the second visit for the day. Thank you Brunei Cyber Security Association for coordinating and EVYD for hosting.



On the same day, our students attended the Brunei Cyber Security Association CySec 2024 and interacted with our Coporate Partner Huawei Singapore and Yang Berhormat, Pengiran Dato Seri Setia Shamhary bin Pengiran Dato Paduka Haji Mustapha, Minister of Transport and Infocommunications as the Minister-in-charge of Cyber Security.



Learning Journey to Brunei Day 3, 19 September

On 19 September, the students visited IGS. Thank you Brunei Cyber Security Association & Wissen International for coordinating and IGS from hosting.



Subsequently, the students also visited Dynamik Technologies. Thank you Brunei Cyber Security Association for coordinating and Dynamik from hosting.



Learning Journey to Brunei Day 4, 20 September

On 20 September, the students visited High Commission Singapore in Brunei. Thank you, High Commissioner, Mr Laurence Bay, for hosting and conducting the dialogue session with the students.



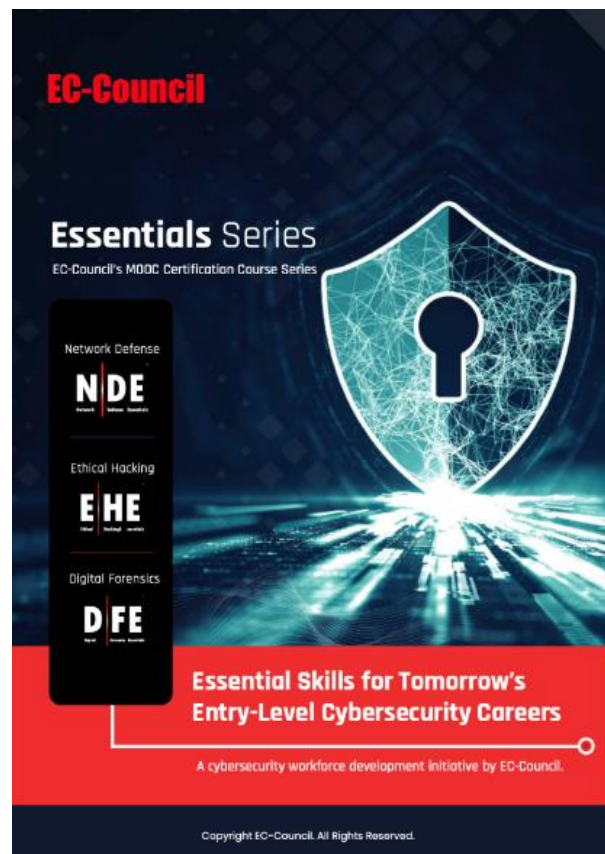
Elevating Cybersecurity Education Through Unprecedented Collaborations

In a pioneering initiative, EC-Council and Wissen have forged a collaboration with AiSP. This collaboration includes a sponsorship of 500 EC-Council Cyber Essentials certification vouchers. These vouchers aim to empower Polytechnic and Institute of Technical Education (ITE) students pursuing cybersecurity programs, enabling them to attain their inaugural industry certificate and commence their journey with EC-Council Essential certificates (NDE, EHE, DFE), thereby initiating their cybersecurity credentialing process.

Visit (<https://wissen-intl.com/essential500/>) and register to start your cybersecurity credentialing journey! Terms & Conditions apply.

About the EC-Council Cyber Essentials Certification

EC-Council's Essentials Series is the first MOOC certification course series covering essential skills in network defense, ethical hacking, and digital forensics. The Network Defense Essentials (N | DE), Ethical Hacking Essentials (E | HE), and Digital Forensics Essentials (D | FE) are foundational programs that help students and early career professionals choose their area of competency or select a specific interest in cybersecurity. The Essentials Series was designed to give students the foundation on which to build and develop the essential skills for tomorrow's careers in cybersecurity. These programs educate learners in a range of techniques across industry verticals, such as securing networks, mitigating cyber risks, conducting forensic investigations, and more.



AiSP Cyber Wellness Programme

Organised by:



Supported by:



In Support of:



The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. There has been an increase in cyber threats, online scams and COVID-19 related phishing activities. With reduced Face-to-Face engagements, the elderly and those with special needs have become more vulnerable to cyber threats. We will reach out to different community groups to raise awareness on the topic of cyber wellness and cybersecurity and participants can pick up cyber knowledge through interactive learning. It is supported by the Digital for Life Fund, an initiative by the Infocomm Media Development Authority (IMDA), that supports digital inclusion projects and activities to help all Singaporeans embrace digital, to enrich lives."



Join us in our monthly knowledge series to learn and pick up tips on Cybersecurity. Visit our website (<https://www.aisp.sg/aispcyberwellness>) to get updates on the latest Cyber tips, Cyber news, activities, quiz and game happenings related to Cyber. Scan the QR Code to find out more.



Scan here for some tips on how to stay safe online and protect yourself from scams



Hear what some of our Professionals have to share. Scan here on Cyber - Use, Identity, Relationship, Citizenship & Ethics.



Have the knowledge and think you are safe? Challenge yourself and participate in our monthly quiz and stand to win attractive prizes. Scan now to take part.



Scan here if you are looking for activities / events to participate in for knowledge exchange / networking / get to know more people / stay protected & helping others.



Want to know more about Information Security? Scan here for more video content.



To find out more about the Digital for Life movement and how you can contribute, scan here.

Contact AiSP Secretariat at secretariat@aisp.sg to find out more on how you can be involved or if you have any queries.

Click [here](#) to find out more!

[back to top](#)

Special Interest Groups

AiSP has set up six **Special Interest Groups (SIGs)** for active AiSP members to advance their knowledge and contribute to the ecosystem are:

- Artificial Intelligence
- CISO
- Cloud Security
- Data and Privacy
- DevSecOps
- Legal Investigative Technology Experts (LITE)

We would like to invite AiSP members to join our **Special Interest Groups** as there are exciting activities and projects where our members can deepen their knowledge together. If you are keen to be part of a SIG, please contact secretariat@aisp.sg



DevSecOps SIG Meetup on 3 September

AiSP held our very first DevSecOps SIG Meetup on 3 September where our SIG members get to network and find out more about the SIG from our SIG EXCO Lead Mr Stanley Eu. Thank you to our Corporate Partner Parasoft, Scantist and our Academic Partner Nanyang Polytechnic for supporting.



Cloud Security Summit on 24 September

More than 120 attendees came for the AiSP Cloud Security Summit 2024 on 24 September where there was insightful sharing on the evolving challenges and opportunities in cloud security. A big thank you to AiSP Patron - SMS Tan Kiat How for gracing the event and sharing valuable perspectives on Evolving Strategies Beyond Cloud Security.

Special thanks to our sponsors, Huawei, Cisco, ONESECURE Asia Pte Ltd, Tenable, Votiro and Wissen International and supporting partners for their unwavering support in making this summit a success. Thank you, Mr Stanley Tsang, Mr Avinash Naduvath, Mr Kevin Li and Dr Weiham Goh for sharing their valuable insights and expertise with the attendees.

We would also like to thank the panellists, Mr Jon Lau, Mr Frank Guo, Prof Steven Wong and SMS Tan Kiat How for the enriching and thought provoking sharing moderated by AiSP EXCO Lead for Cloud Security SIG, Mr Dennis Chan. Thank you everyone for playing a part in contributing to the success of the summit and we hoped the attendees have benefitted greatly from the event!



AiSP LITE SIG Meetup - Inside the Lab: A Day in the Life of a Digital Forensic / e-Discovery Specialist on 3 October



AiSP LITE SIG Meetup - Inside the Lab: A Day in the Life of a Digital Forensic / e-Discovery Specialist



Chua De Hui
LITE SIG Co-Lead
AISIP
Director
Deloitte Forensic Southeast Asia
Moderator



Jacky Ang
Digital forensics analyst in a
TECH MNC
Panellist



Mohamad Ridzuan
Digital Forensic Examiner
Home Team Science and
Technology Agency
Panellist



Shirley Liew
Senior Consultant
FTI Consulting
Panellist

Organised By:



Supported by:



📅 3 Oct 2024, Thurs
🕒 6PM - 8.30PM
📍 JustCo @ Marina Square

Register Here:



AiSP has set up a Special Interest Group - **Legal Investigative Technology Experts (LITE)**.

Our Vision is to provide a platform for AISIP members who are keen in the investigations space, specialising in the realms of digital forensic / e-Discovery, to participate in and benefit from each other's expertise, so as to create a vibrant and dynamic ecosystem.

Join us for an enlightening panel discussion that delves into the daily responsibilities and challenges faced by Digital Forensic / e-Discovery specialist in the public sector, consulting, and as an in-house practitioner. This session will provide a behind-the-scenes look at the critical work conducted by these specialists in the realm of the digital, legal, and investigative landscape.

Panel Discussion

Inside the Lab: A Day in the Life of a Digital Forensic / e-Discovery Specialist

This discussion will feature a diverse panel of digital forensic / e-Discovery specialists with varied expertise from the different sectors, offering a comprehensive view of the profession. Whether you're a student aspiring to enter the field, a professional seeking to understand the digital investigative landscape better, or simply curious about the work behind the scenes, this session promises to be both informative and engaging.

Moderator:

Chua De Hui

De Hui is a Director at Deloitte Forensic Southeast Asia, bringing over a decade of expertise in Digital Forensics, eDiscovery, and investigative advisory services across Southeast Asia's diverse economies. Throughout his career, De Hui has successfully led and managed a wide array of

engagements, including complex digital forensic investigations, eDiscovery reviews, and as well as execution of Search Orders across Singapore and Malaysia.

In addition to his role at Deloitte, De Hui is currently the co-lead of Legal Investigative Technology Experts, where he hopes to contribute new ideas and attract young talents to the industry.

Panelists:

Jacky Ang

With close to 4 years of DFIR experience, Jacky is currently working in-house as a digital forensics analyst in a TECH MNC and has been in both the government and private sector. He specialises mainly in Windows forensics and holds a GCFA certification. During his free time, he likes to hunt for good food, watch football matches and also read up on threat intel, DFIR blogs and general cybersecurity news to stay updated.

Mohamad Ridzuan

Ridzuan kicked off his digital forensics journey in 2016 with the Singapore Police Force and later transitioned to the newly established Home Team Science and Technology Agency (HTX). Specializing in mobile and drone forensics, and now dabbling in malware forensics, he's all about diving deep into the digital world.

Armed with certifications like GCFE, GCFA, GASF, and GREM, Ridzuan is always on the hunt for new knowledge, whether it's through training, education, or hands-on experience with the latest forensic tools.

When he's not unravelling digital mysteries, you'll find him obsessing over Capture the Flag (CTF) challenges.

Shirley Liew

Shirley is a Senior Consultant in the Technology Segment at FTI Consulting. As a digital forensic and e-Discovery consultant, she specializes in forensic collection, data analysis and assist in expert reporting of digital evidence. Shirley has been involved in matters relating to Intellectual Property (IP) theft, information leakage, bribery and corruption, and other employee-related misconduct. She has more recently attained GIAC Certified Forensic Examiner (GCFE), and is part of their advisory board.

Date: 3 October 2024, Thursday

Time: 6PM – 8.30PM

Venue: JustCo @ Marina Square

Registration: <https://www.eventbrite.sg/e/aisp-lite-sig-meetup-tickets-979651402717>

*AiSP members who would like to bring a non member for the event can reach out to secretariat@aisp.sg for a 50% discount code.

The Cybersecurity Awards



Thank you for your support! The Cybersecurity Awards 2024 nominations has ended and the awards ceremony will be on 7 November 2024.

Professionals

1. Hall of Fame
2. Leader
3. Professional

Students

4. Students

Enterprises

5. MNC (Vendor)
6. MNC (End User)
7. SME (Vendor)
8. SME (End User)



ORGANISED BY



SUPPORTED BY



SUPPORTING ASSOCIATIONS



SINGAPORE



PLATINUM SPONSORS



GOLD SPONSORS



[back to top](#)

Regionalisation

SEA CC Webinar – Ladies in Cyber on 5 September

The South East Asia Cybersecurity Consortium has been organising a series of webinars leading up to the SEA CC Forum 2024 happening on 18 September 2024 in Brunei. On 5 September, the webinar was held on Ladies in Cyber as part of the International Women in Cyber Day (1 September). Thank you Brunei Cyber Security Association, Malaysia Board of Technologists and WiSAP (Women in Security Alliance Philippines) for sending representatives to speak at the webinar. Thank you our Corporate Partner, Ms Vivien Tan from Cybersafe for representing Singapore to speak at the webinar.



AJCCA Conference on 17 October



The International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC) was held in 2023 in Tokyo. At the Conference, 8 associations of Southeast Asian Nations members and Japan agreed to a private sector cybersecurity collaboration and the

[back to top](#)

ASEAN Japan Cybersecurity Community Alliance (AJCCA) was established. This year, AJCCA Conference 2024 will be held in Singapore on 17 October 2024 and will be hosted by AiSP. As such we would like to invite our AiSP Members to join us in the conference.

The ASEAN Japan Cybersecurity Community Alliance (AJCCA) is a collaborative initiative formed by nine leading cybersecurity communities from ASEAN nations and Japan. AJCCA is dedicated to enhancing cybersecurity capabilities, information sharing, and mutual support among its member nations to address the evolving challenges in the digital landscape.

AJCCA Vision

"A dynamic and resilient cybersecurity community in our region through trustworthy and respectful collaboration"

AJCCA Mission

1. Facilitate Exchanges Among Organizations :

Recognizing the importance of diverse perspective and experiences in tackling cyber threats, the AJCCA aims to deepen mutual understanding , interactions and collaborations across member countries about cybersecurity governance and operations.

2. Exchange Information on Cyber Threats for better cyber resilience:

A critical component of the alliance is the sharing of intelligence regarding cybersecurity threats, incidents, and solutions prevalent in each member country. This information exchange is pivotal in pre-empting and mitigating cyber-attacks.

3. Improve and Enhance Sustainable Cybersecurity Capacity:

The alliance focuses on building trust , nurturing capacities and enhancing security awareness among its members. This involves joint training programs, workshops, and seminars to equip members with the latest cybersecurity knowledge and skills

Event Details

Date: 17 October 2024 (Thursday)

Time: 9am to 4.30pm

Venue: Suntec Convention and Exhibition Centre Level 3

Register [here](#) and choose the below option for special price.

Digital For Life

Digital for life Mooncake festival with Kampong Chai Chee Residents' Network & Huawei on 14 September

AiSP was at the Mid-Autumn Celebration organized by Huawei together with Kampong Chai Chee Bedok Town Centre Residents' network held on 14 September with more than 80 residents. The residents had a fun time making lanterns with red packets, guessing riddles and designing mooncakes coupled with delicious food at the event. Thank you, Grassroot Advisor to Kampong Chai Chee & AiSP Patron - SMS Tan Kiat How for gracing the event and distributing mooncakes and interacting with the residents! AiSP EXCO Lead for Cyberwellness and Huawei CSPO, Mr Dennis Chan was also at the event to interact with the residents and celebrate the festive season by giving out mooncake. We hope the residents had a great time of celebration and enjoyed the time of food and activities as much as we did. Thank you, Huawei, for the sponsorship to make this event a great success.



[back to top](#)

Digital for Life at Jurong Spring CC on 28 September

AiSP was invited to attend the opening of the Digital Community Hub at Jurong Spring CC on 28 September. AiSP EXCO Lead, Mr Dennis Chan joined Adviser SPS Shawn Huang and 2nd Adviser Dr. Hamid Razak for the opening ceremony. The residents had a fun filled day of learning digital skills and activities. Thank you IMDA for inviting us!

[back to top](#)

Upcoming Activities/Events

Ongoing Activities

Date	Event	Organiser
Jan – Dec	Call for Female Mentors (Ladies in Cyber)	AiSP
Jan – Dec	Call for Volunteers (AiSP Members, Student Volunteers)	AiSP

Upcoming Events

Date	Event	Organiser
1 Oct	QiSP Workshop	AiSP
2 Oct	Cyber Security and Data Protection Day 2024	Partner
3 Oct	LITE SIG Meetup	AiSP
7 Oct	Learning Journey to Grab by RP Students	AiSP & Partner
9-10 Oct	SMEICC 2024	Partner
9-10 Oct	Cyber Security World Asia / Cloud Expo	Partner
15-17 Oct	Govware	Partner
17 Oct	Asean-Japan Cybersecurity Community Alliance Conference	AiSP & Partner
22 Oct	NHG Cybersecurity Awareness Sharing	Partner
24 Oct	URA Growth Nodes Exhibition	Partner
2-3 Nov	Digital for life Festival by IMDA	Partner
5 Nov	CISO Meetup – What is the role of a CISO	AiSP & Partner
6-7 Nov	STACK 2024 Developer Conference	Partner
6-8 Nov	Singapore FinTech Festival (SFF) 2024	Partner
7 Nov	TCA24 Gala Dinner	AiSP
11-14 Nov	Cisco Live 2024 Melbourne	Partner
14 Nov	CPP Event with Wizlynx	AiSP & Partner
14 Nov	CISO Canberra 2024	Partner
19 Nov	SVRP Awards Ceremony	AiSP
19-20 Nov	CISO New Zealand 2024	Partner
26-28 Nov	Australian Cyber Conference Melbourne 2024	Partner
27-28 Nov	CDIC Conference 2024 Bangkok	Partner

***Please note events may be postponed or cancelled due to unforeseen circumstances*

CONTRIBUTED CONTENTS

Article from CISO SIG

Christopher Lek is a seasoned cybersecurity professional with over 20 years of experience in telecommunications, financial institutions, and global conglomerates. He has held various roles, including governance, risk management, security architecture, and cyber defence. Currently, he leads the cybersecurity team at Nanyang Technological University and has been a three-time winner of the Top 30 Cybersecurity Executives award for his contributions to business value, leadership, and his ability to drive change in the CSO30 ASEAN awards

Introducing CISO with a deep interest in cybersecurity

Chris currently leads the Cyber Security Team at Nanyang Technological University overseeing the cyber security function for the university across administration, teaching learning and research. He served as the founding Director of Cybersecurity for NTU, overseeing the expansion of the team with specializations in governance, engineering, and cyber defence. He has led various security initiative effort over the last few to improve the security posture for the university. He had also led the team to attain ISO 27001 and Cyber Trust Mark (Advocate) certifications for the university's critical IT services.

What brought you to the Cybersecurity industry?

During my earlier career in the internet service provider, I encountered various security incidents (e.g., hacking, DDoS) which inspired me to pursue a career in cyber security. My first stint in cyber security started as a team lead in the national critical payment system where I was responsible for overseeing network and security operations to secure billions of dollars of interbank transactions. At the same time, I was introduced to the SIG² GTEC Labs, where I was exposed to capture the flag competitions and honeypots, which further ignited my interest in this domain. Further experience with global conglomerates like Sony and General Electric put me through the trenches of advanced persistent threats and dealing with nation-state actors. This has been a humbling experience and solidified my belief that attacks are real, and we need to be resilient.

What were your defining moments in this industry, and factors or guidance that helped you achieve them?

One of the most defining moments was the experience with the Sony Pictures breach during Thanksgiving Day in 2014. The attack, believed to be carried out by North Korean state-sponsored hackers, resulted in the theft of sensitive company data, including employee personal information and unreleased movies. Many of our assets were wiped out, and the organization was basically brought to a halt. As the saying goes, 'What

[back to top](#)

doesn't kill you makes you stronger.' It was in the aftermath of this incident that cyber security received strong support from top management. Numerous initiatives and transformations occurred to strengthen cyber security resilience and capabilities. This also provided opportunities to work with great colleagues to enhance our defence against advanced persistent threats. I am grateful to have been mentored by my bosses and to have built strong camaraderie with fellow global team members during my working experience with Sony.

What is it that you love most about your role?

Making a positive impact to the organisation with persistency and the grit to get back from any setback

What are some of the trends you have seen in the market lately, and what do you think will emerge in the future?

The use of Deepfake technology is increasing, which will make social engineering attacks more complex and convincing. The adoption of quantum-resistant encryption is also gaining more attention as hackers are exploring ways to break traditional encryption algorithms.

What do you think is the role of CISO?

The role of a CISO is multifaceted. Not only are you required to be technically proficient, but you also need to have strong business acumen to navigate complex organizations. This requires a combination of hard skills (technical) and soft skills (communication, stakeholder management) to succeed in this role.

What can we do to encourage more people to join the cybersecurity sector?

I don't think there's a lack of interest among the younger generation in joining this sector. However, I believe we need to let them know that if they're keen to embark on a cyber security career, they need to develop critical thinking skills, a passion for learning, and the ability to be resilient against any adverse situation.

What do you want to achieve or contribute to the Cybersecurity Ecosystem?

I am humbled that over the past few years, the NTU cyber security team's efforts in cyber security awareness and transformation have been recognized through various awards. This is attributed to a dedicated team of members and my management's support. NTU is currently a member of the CSA cyber security awareness alliance, and we hope to continue to promote and enhance awareness and adoption of good cybersecurity practices among members of the public and organizations in Singapore. In 2024, NTU successfully established the newly minted student's cyber security club, and I am honored to be the advisor. I hope to continue inspiring the younger generation to pursue their passion and excel in their cyber security careers.

Any advice for the Cybersecurity Professionals?

It is important to understand your strength and shortcomings and to be self-aware. Build on your strength and make a concerted effort to strengthen your weakness. Continuous learning and curiosity are essential and always ask "why" to delve deeper into concepts and challenges.

Collaboration is another crucial aspect as cybersecurity is a team sports. Work effectively with colleagues from various departments and backgrounds. To achieve collaborative cyber defence, we must breakdown organizational silos and promote open communication. The world of cybersecurity is always changing, so we must continue to be flexible, accept new technology, and be ready to take on new problems.

Article from AI SIG

Artificial Intelligence 101

Artificial intelligence (AI), as a discipline, is not new. However, it has gained renewed popularity in recent times due to the astounding accomplishments of large language models such as ChatGPT and Gemini. These complex models are trained on very large datasets and use intensive resources to learn from this data such as GPU clusters as well as human feedback. However, not all forms of AI have such hefty requirements. In fact, early forms of AI were much smaller in size and complexity than the models we see today. The term AI was introduced at a conference in 1956, and the field has a long and storied history, having gone through multiple summers and winters.

Research in AI resulted in some successes as early as the 1960s, for example with the natural language processing program ELIZA exploring communication between man and machine. ELIZA adopted a pattern matching and substitution method. Nevertheless, it was sophisticated enough to produce intelligent responses that were capable of deceiving early users of the program. Another important approach adopted by early AI researchers was to attempt to replicate the decision-making process of a human expert. Introduced by Edward Feigenbaum, these expert systems would collect information from a human expert and use this information for advising non-experts. There were two main components to expert systems – (1) a knowledge base representing information about the world, and (2) an inference system utilising logic rules and formal statements to create new knowledge. These systems were used in industries and enjoyed some success; it was probably best exemplified by the victory of Deep Blue over Gary Kasparov, who was the world's best chess player in 1997. Deep Blue combined the knowledge provided by chess experts with an efficient search algorithm and powerful processors, enabling it to evaluate 200 million chess positions per second.

These early AI programs attempted to replicate human intelligence by using a collection of rules, and implicitly assumes that the problem can be formalised based on these rules. While this may be true of certain tasks, others such as image recognition or language

[back to top](#)

translation are less amenable to this approach. For such tasks, a better approach may be for the system to learn from the data and to adjust and adapt itself to better achieve its objectives without being explicitly programmed. These algorithms come under the subset of AI known as machine learning. Due to the automated nature of machine learning algorithms, they can quickly learn from large amounts of data and can identify patterns that are not obvious even to experienced analysts. Machine learning models can vary widely in terms of complexity and size.

A popular subset of machine learning today is deep learning, which builds on a particular machine learning model called neural networks. The inspiration for this model comes from nature, specifically the workings of the human brain, although the abstract representations found in the AI model today do not exactly mirror their biological counterpart. Deep learning models, by virtue of their large and complex architectures, can learn from large and complex datasets without requiring advanced preprocessing of the data. Classical machine learning models, on the other hand, usually require domain specific knowledge to extract relevant features from the data to improve model performance. Deep learning models have been tremendously successful in the fields of computer vision and natural language processing, outperforming their classical counterparts and are also the foundation of impressive generative models such as ChatGPT or DALL-E.

Broadly speaking, most machine learning tasks can be divided into supervised and unsupervised learning. The crucial distinction between these two tasks is the availability of labels. A label is an actual classification for each sample, for example whether an email is spam or ham, or whether a file is malware or not. When such labels are available, the task is one of supervised learning, and the AI tries to learn the relationship between the inputs (such as the presence or absence of certain words in an email) and the labels (such as whether the email is spam or ham). For such tasks, the machine learning process normally undergoes two phases: (1) a training phase where the model is presented with the correctly labelled training data and 'learns' from this data; and (2) a testing phase where the fully trained model is fed with 'unseen' data i.e. data not in the training data but for which the labels are known, and the model's performance is evaluated. Some examples of supervised machine learning models include distance-based methods such as K-Nearest Neighbours, probabilistic methods such as Naïve Bayes, deep learning neural network architectures such as convolutional neural networks and transformers, and ensemble methods which use a collection of simpler models to improve performance.

For evaluation of supervised learning models, the most intuitive metric to use is accuracy, which essentially measures the overall percentage of correctly predicted samples. However, for some problems where the number of samples in the output classes are not evenly distributed, such a measure may not be reflective of the actual performance of the model. For example, in the context of cybersecurity related problems, malicious events are usually much rarer than benign ones. Thus, a high accuracy based on overall percentage would be misleading; the model would be able to give good results just by always predicting the majority class, as the small number of malicious events that are incorrectly predicted will not affect the accuracy score greatly. In this case, other

performance metrics such as precision (the percentage of correct predictions out of all malicious samples), recall (the percentage of correct predictions out of all maliciously predicted samples) or other such metrics may be informative.

For unlabelled data, unsupervised learning methods can be used. These methods attempt to discover patterns or find some underlying structure within the unlabelled dataset. Clustering algorithms like k-means clustering, group the data based on similarity, and these groups can be further studied by a domain expert to identify anomalies that do not belong to any group or to classify new data into one of the groups. Alternatively, deep learning architectures such as autoencoders can be trained to recreate the original input from a lower dimensional representation of the input. Once trained, autoencoders can reconstruct the input accurately for non-anomalous data but will fail for outliers and can therefore be used for anomaly detection. Other unsupervised anomaly detection methods include tree-based methods such as isolation forests which uses the number of splits in the trees to identify anomalies.

In some situations, a combination of both supervised and unsupervised learning can be used in what is called semi-supervised learning. This normally applies to cases where there is limited labelled data but large amounts of unlabelled data. The goal of semi-supervised learning is the same as that of supervised learning, but in this case, the small set of labelled data is used to create machine generated labels for the unlabelled data which can then be used to enhance the performance of the overall model. Another subset of machine learning that differs from supervised and unsupervised learning is reinforcement learning. There are three key components in reinforcement learning – the environment, action and reward. An agent repeatedly interacts with a simulated environment, and in the process receives rewards or penalties depending on the actions taken. By exploring the simulated environment in this fashion, the agent learns the 'best' moves to take when in a given state and optimises for the long term instead of short-term rewards. An important requirement for the success of reinforcement learning is the creation of realistic simulation environments. One such platform provided by Microsoft is CyberBattleSim, which simulates attack and defence cyber-agents (<https://www.microsoft.com/en-us/research/project/cyberbattlesim/>). The attacker evolves in the network via movements to exploit existing vulnerabilities while the defender attempts to contain the attacker and evict it from the network. Reinforcement learning can be used to learn the appropriate strategies for an attacker to infiltrate all PCs in a network environment, or to develop effective defence strategies.

With digital transformation changing the way we live and work, addressing cybersecurity threats has become increasingly important. Attackers are constantly finding new ways to attack systems, creating a dynamic and changing threat landscape that may not be amenable to rule based methods. The strengths of machine learning, as a fast and automated method of learning from data, appear to make it well suited for tackling problems in the cybersecurity domain. However, challenges remain, such as the need for large and diverse datasets, data drift, interpretability of AI models and difficulties in handling both zero-day attacks and AI-based adversarial attacks created specifically to escape detection. Furthermore, the trend from narrow intelligence (AI developed for specific tasks) to a more general intelligence, such as the multimodal language models

that can perform multiple tasks, will open new opportunities and threats in the cybersecurity domain. While there is still a discrepancy between the research potential and practical deployment of AI-based cybersecurity solutions today, it is likely that this gap will narrow in the near future.

Contact Information:
Brandon Ooi (Dr)
School of Information Technology
Nanyang Polytechnic
E-mail: brandon_ooi@nyp.edu.sg

Article from Cloud Security Summit Sponsor - Tenable

Tenable Named a CRN 2024 Cloud 100 Company Tenable continues to innovate and advance its market-leading cloud security solution

Tenable®, the Exposure Management company, today announced that CRN®, a brand of The Channel Company, has named Tenable to its annual Cloud 100 list. This list honors the 100 leading cloud companies for 2024 across five key categories: infrastructure, monitoring and management, storage, software and security.

CRN's Cloud 100 list spotlights technology suppliers for their commitment to channel partners, as well as their demonstrated innovation in cloud-based technology development. This list is the trusted resource for solution providers looking for technology vendors best positioned to support their cloud product and service's needs.

Tenable is a channel-first company, providing partners with the tools and resources to mature their security programs or those of their customers. Tenable Cloud Security is the company's market-leading, unified cloud security solution. It simplifies the identification and remediation of cloud risk, from code to cloud and across multi-cloud environments. The easy-to-use solution puts context and actionable intelligence front and center, enabling security teams to remediate issues rapidly regardless of cloud security expertise.

Tenable Cloud Security is available as a standalone solution and as part of the Tenable One Exposure Management Platform, a cloud-based exposure management platform. Tenable One delivers contextual risk visibility, so security teams can focus on likely attacks and accurately communicating cyber risk to support optimal business performance.

"Tenable's platform takes the painstaking complexity out of cloud security," said Shai Morag, SVP and General Manager, Cloud Security, Tenable. "Cloud environments require more time and resources from security professionals than traditional IT infrastructure, so Tenable Cloud Security was built with user experience at the forefront. We offer a full-stack approach with broad breadth and depth of coverage – from identities, networks, workloads, code, and data – providing customers with a complete picture of their exposure to cyber risk."

In October 2023, Tenable completed the acquisition of Ermetic, an innovative cloud-native application protection platform (CNAPP) company and a leading provider of cloud infrastructure entitlement management (CIEM). Ermetic was named to CRN's 2023 Cloud 100 list.

"As migration to the public cloud and cloud-based software accelerates, enterprises increasingly depend on innovative, secure cloud services to harness the cloud's agility and scalability," said Jennifer Follett, VP, US Content and Executive Editor, CRN, The Channel Company. "The companies selected for this year's Cloud 100 list demonstrate a strong commitment to supporting cloud computing solution providers with leading-edge products and services. Congratulations to those on this year's list! We look forward to seeing how they propel innovation and channel success in cloud computing throughout the year ahead."

CRN's Cloud 100 list will be featured in the February 2024 issue of CRN magazine and online at www.crn.com/cloud100.

More information on Tenable Cloud Security is available at www.tenable.com/products/tenable-cloud-security.

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at tenable.com.

###

Media Contact:

Tenable

tenablepr@tenable.com

Article from Cloud Security Summit Sponsor - Wissen



The Blueprint for Securing the Hybrid Cloud: Essential Cloud Security Training

Instead of restricting themselves to only one cloud provider, many organizations are choosing a so-called “hybrid” cloud approach. In hybrid cloud computing, a single business uses multiple computing environments, including at least one public cloud.

A hybrid cloud setup may combine multiple public and private clouds or the cloud and on-premises infrastructure.

While the hybrid cloud has many applications and benefits, it also presents additional security complications. Knowing how to protect hybrid cloud environments is crucial to cloud security training. This article will outline a blueprint for securing the hybrid cloud.

4 Benefits of the Hybrid Cloud

Cloud computing has gone from being a cutting-edge technology to a best practice for businesses of all sizes and industries. The 2022 Flexera State of the Cloud survey found that all companies who responded were using at least one public or private cloud, and 80 percent of companies have a hybrid cloud environment (Flexera, 2022).

With the vast majority of businesses now using the hybrid cloud, what are its applications and advantages? Below are just a few benefits of a hybrid cloud setup:

- **Flexibility:** A hybrid cloud allows an organization to choose the most appropriate infrastructure for each workload or application. For example, one application

[back to top](#)

might be more efficient or cost-effective in the cloud, while another is required to run on-premises due to regulatory compliance issues.

- **Scalability:** A hybrid cloud allows an organization to easily scale its resource consumption up or down in the cloud as needed. This can be useful during periods of unexpectedly high demand or when the organization no longer needs certain resources.
- **Availability and disaster recovery:** A hybrid cloud can limit the damages and business disruption in the event of downtime or disaster. If one cloud environment is temporarily unavailable, others can pick up the slack.
- **Integration:** A hybrid cloud allows companies to easily integrate their existing on-premises infrastructure with a public cloud. This can be useful for organizations that want to leverage the cloud while maintaining ultimate control over certain aspects of their IT infrastructure.

3 Hybrid Cloud Security Training Challenges

The hybrid cloud has additional security challenges that may not be present in other environments, such as a single cloud provider or an on-premises setup. Below are some unique concerns that hybrid cloud users should be aware of during cloud security training:

- **Standardizing policies and procedures:** AWS security questions will differ from Azure security and GCP security issues. Businesses that use multiple cloud providers in their hybrid cloud environment must consider how their security policies and procedures will carry over between these providers. As much as possible, security protocols should be standardized across each cloud and between the cloud and on-premises.
- **Monitoring and observability:** Monitoring is an essential practice for businesses that use the cloud, helping detect and respond to events. However, different providers offer their own tools for monitoring the events inside a cloud environment: Amazon CloudWatch, Azure Monitor, and Google Cloud Monitoring, to name a few. Users of the hybrid cloud need a way to integrate and observe all these logs and data simultaneously.
- **Compliance issues:** Data privacy and security regulations such as HIPAA, GDPR, and CCPA restrict how businesses can collect, process, store, and analyze sensitive personal information. They also enact harsh penalties in the event of a data breach (GDPR, 2019). With data potentially flowing between multiple clouds in a hybrid cloud environment, organizations must protect this information from a potential cloud data breach while ensuring compliance with applicable laws and standards.

The Blueprint to Secure the Hybrid Cloud

Hybrid cloud environments are more technically complex than a single cloud, making them harder to protect. Businesses should follow the hybrid cloud best practices below for cloud security training:

1. **Deal with interoperability:** Interoperability—the ability of IT resources in different clouds to communicate and work together—is a crucial concern for the hybrid cloud. A robust solution for hybrid cloud security will consider the system's interoperability when configuring and monitoring assets across the organization's cloud landscape.
2. **Use automation:** The hybrid cloud typically occupies a larger footprint than a single cloud or on-premises environment, making manual observation impossible. Automated tools can produce and analyze logs, scanning for vulnerabilities and anomalies, while the human IT team focuses on the bigger picture.
3. **Exercise the principle of least privilege:** The larger footprint of the hybrid cloud also leads to more significant concerns about identity and access management. Organizations must ensure that users can only access the resources necessary to do their jobs across the hybrid cloud environment, a concept known as the principle of "least privilege."
4. **Keep processes uniform:** With multiple cloud environments, it's easy for organizations to have divergent security configurations—for example, neglecting to apply changes across all providers. To strengthen cloud security, processes and policies should be kept as uniform as possible across the entire hybrid cloud.
5. **Use data protection and compliance:** Organizations must comply with any data privacy and security regulations that concern them, such as HIPAA, GDPR, CCPA, or PCI DSS. To avoid data leakage, information should be protected with techniques such as encryption, which is a cloud security best practice (Puzas, 2022). This is especially true for a hybrid cloud setup, where information may be frequently transferred between cloud providers.
6. **Secure endpoints and workstations:** The more endpoints connected to the hybrid cloud, the larger the attack surface becomes. Computers, mobile phones, routers, and other devices that use the hybrid cloud should all be protected with security tools such as firewalls and EDR (endpoint detection and response) software.
7. **Create backup and disaster recovery strategies:** The cloud is already the favored solution for backing up information because cloud providers store data in multiple physical locations. Businesses should take advantage of the additional resilience and reliability of the hybrid cloud to store essential data with multiple cloud providers and to develop a disaster recovery plan that can account for this setup.

How to Secure a Hybrid Cloud Environment

The hybrid cloud has many advantages, but hybrid cloud security presents several challenges that must be surmounted. Still, by following a robust hybrid cloud security blueprint, organizations can protect their hybrid cloud environments and dramatically lower the risk of cyberattacks.

How can companies get started with hybrid cloud security training? Cloud providers like Google offer certifications, such as Google Cloud security engineer, but these programs are only intended for learning about a single cloud solution—not a hybrid cloud setup that uses multiple providers.

Businesses need a hybrid cloud security program that is both vendor-neutral and vendor-specific. Students should learn about general cloud security practices, technologies, frameworks, and principles without reference to any one provider. However, they also need practical, vendor-specific knowledge to apply what they've learned in the real world.

That's precisely what EC-Council's [Certified Cloud Security Engineer \(C | CSE\)](#) program has to offer. The C | CSE certification provides the perfect blend of vendor-neutral and vendor-specific approaches to cloud security, teaching theoretical and practical skills. Students who obtain a C | CSE certification will be well-prepared to assume the job roles and responsibilities of cloud security professionals.

Ready to start your career in cloud security and looking for the best cloud security certification? Email enquiry@wissen-intl.com for more information!

Sources

Flexera. (2022). State of the Cloud Report. <https://info.flexera.com/CM-REPORT-State-of-the-Cloud>

GDPR. (2019, February 13). What are the GDPR Fines? <https://gdpr.eu/fines/>

Puzas, D. (2022, October 13). What is Cloud Encryption?

CrowdStrike. <https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-encryption/>

About the Author

David Tidmarsh is a programmer and writer. He's worked as a software developer at MIT, has a B.A. in history from Yale, and is currently a graduate student in computer science at UT Austin.

Article from SVRP 2023 Gold Winner, Elton Tay Chee Hean [NYP]



How do you think SVRP has directly impacted your cybersecurity journey?

SVRP has helped me to be recognized for my efforts in contributing to the field of Cybersecurity through my various forms of volunteering work. Being able to share my passion and love for cybersecurity while educating the future generation of cybersecurity professionals has been something I pride myself in doing since I entered this field. Being recognized for my efforts and contributions is an added bonus to me and makes me stand out better.

How has SVRP inspired you to contribute to the cybersecurity field?

Being recognised for my efforts in contributing to this field has been an added bonus to me. I always believe in giving back to the society. SVRP has inspired me to up my game and contribute more to this field, to stand out from the other candidates. Having won Silver last year, I have continually looked for opportunities to volunteer and contribute more to the industry, and I have contributed significantly more in this year as compared to the last.

What motivates you to be a student volunteer?

Cybersecurity is a field that I have always been interested in and have been specializing in for the past 5 years. With the increasing demand of security in today's world, it is important that we can meet the rising demand of cybersecurity professionals. Being a student volunteer allows me to train the future generation of cybersecurity professionals, share my passion and love for this field, and make a impactful contribution to the field.

How would you want to encourage your peers to be interested in cybersecurity?

It is important that we show them, through real world examples, the implications when cybersecurity is not properly implemented. This can range from data breaches, Denial of Service Attacks, or any attack that causes undesirable implications to them as a

[back to top](#)

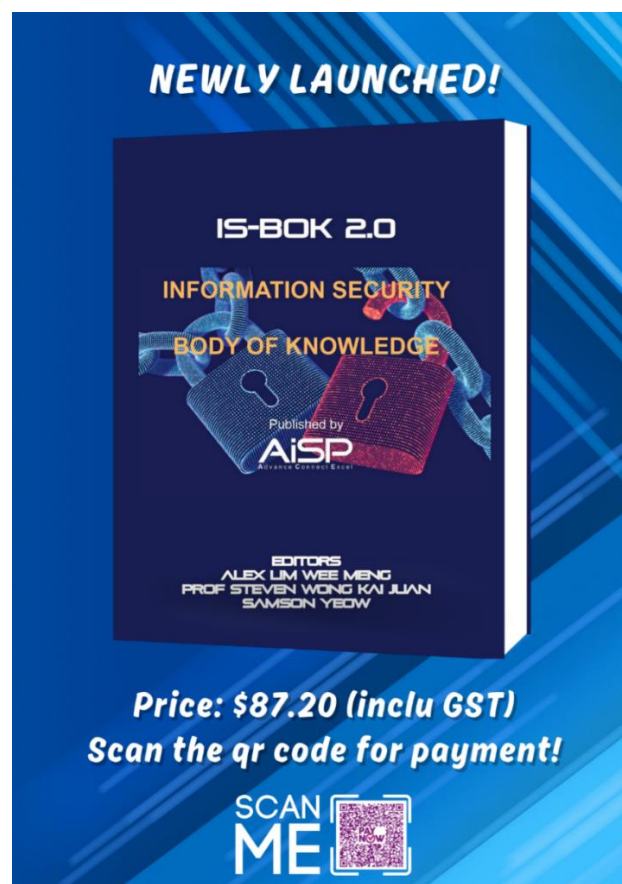
consumer. Through making them realise the importance of cybersecurity in ensuring that consumers like them have a safe and pleasant experience, many will then be motivated to work in this field to protect and serve the public.

PROFESSIONAL DEVELOPMENT

Qualified Information Security Professional (QISP®)

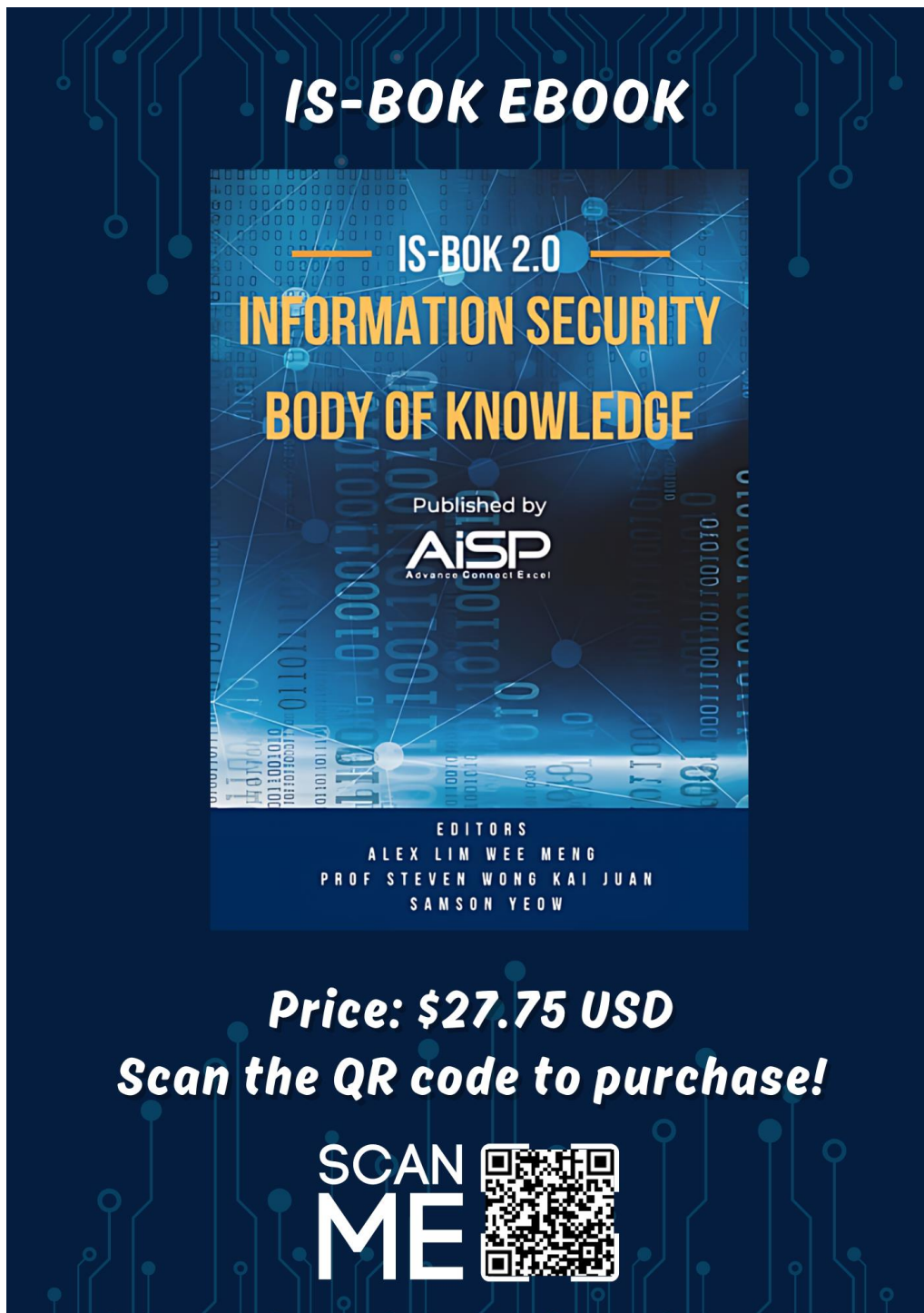
Body of Knowledge Book (Limited Edition)

Get our **Limited Edition** Information Security Body of Knowledge (BOK) Physical Book at **\$87.20 (inclusive of GST)**.



Please scan the QR Code in the poster to make the payment of **\$87.20 (inclusive of GST)** and email secretariat@aisp.sg with your screenshot payment and we will follow up with the collection details for the BOK book. **Last 30 books for sale!**

Body of Knowledge E Book



IS-BOK EBOOK

IS-BOK 2.0


**INFORMATION SECURITY
BODY OF KNOWLEDGE**

Published by
AiSP
Advance Connect Excel

EDITORS
ALEX LIM WEE MENG
PROF STEVEN WONG KAI JUAN
SAMSON YEOW

Price: \$27.75 USD

Scan the QR code to purchase!

SCAN ME 

Online Course launched on 1 March 2024!

QISP Exam Preparatory E-Learning Course

Prepare for QISP Exam via E-Learning Anytime, Anywhere!

Our e-learning program is perfect for those who want to prepare for the QISP Exam based on AiSP IS-BOK domains. With access for 12 months, you can study at your own pace on our beautifully designed and responsive e-learning platform.

Grab the exclusive launch offer at SGD 499 nett!

Special price of SGD 429 nett for AiSP members!

- Governance and Management
- Physical Security and Business Continuity
- Security Architecture and Engineering
- Operation and Infrastructure Security
- Software Security
- Cyber Defense

WISSEN Cyber Security Competency Development | enquiry@wissen-intl.com | www.wissen-intl.com

The QISP examination enables the professionals in Singapore to attest their knowledge in AiSP's Information Security Body of Knowledge domains. Candidates must achieve a minimum of 50-64% passing rate to attain the Qualified Information Security Associate (QISA) credential and 65% and above to achieve the Qualified Information Security Professional (QISP) credential.

Our highly responsive e-learning platform will allow you to learn anytime, anywhere with modular courses, interactive learning and quizzes. Complete the course in a month or up to 12 months! Enjoy lean-forward learning moments with our QISP/QISA preparatory e-learning course. Receive a certificate of completion upon completion of the e-learning course. Fees do not include QISP examination voucher. Register your interest [here!](#)

MEMBERSHIP

AiSP Membership

Complimentary Affiliate Membership for Full-time Students in APP Organisations

If you are currently a full-time student in the IHLs that are onboard of our [Academic Partnership Programme \(APP\)](#), AiSP is giving you complimentary Affiliate Membership during your course of study. Please click [here](#) for the application form and indicate your student email address, expected graduation date and name of your institution in the form.

Complimentary Affiliate Membership for NTUC Members

AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 2024) from 1 Jan 2024 to 31 Dec 2024. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. [This does not include Plus! card holder \(black-coloured card\), please clarify with NTUC on your eligibility.](#)

On [membership application](#), please do not email your personal data to us via email if your information or attachment is not password-protected. Please send us your password via [Telegram](#) (@AiSP_SG).

Once we receive confirmation from NTUC on the validity of your NTUC membership, AiSP would activate your one-year complimentary AiSP Affiliate membership.

CPP Membership



Join our Corporate Partner Programme
for exclusive benefits and partnership with AiSP!

Contact AiSP Secretariat for the benefits and corporate
pricing at secretariat@aisp.sg

For any enquiries, please contact secretariat@aisp.sg

[back to top](#)

AVIP Membership

AiSP Validated Information Security Professionals (**AVIP**) membership helps to validate credentials and experience for IS-related work including cybersecurity, professional development, and career progression for our professionals.

Membership Renewal

Individual membership expires on 31 December each year. Members can renew and pay directly with one of the options listed [here](#). We have GIRO (auto - deduction) option for annual auto-renewal. Please email secretariat@aisp.sg if you would like to enrol for GIRO payment.

Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!

Please check out our website on [Job Advertisements](#) by our partners. For more updates or details about the memberships, please visit www.aisp.sg/membership.html

AiSP Corporate Partners



FORTINET



VECTRA

**Veracity
Trust Network**

VOTIRO

**wizlynx
group**

WISSEN
Cyber Security Competency Development

xcellink.pte.ltd.
completing your technology chain

YesWeHack

Visit https://www.aisp.sg/corporate_members.html to know more about what our Corporate Partners (CPP) can offer for the Cybersecurity Ecosystem.

AiSP Academic Partners

ITE
Institute of Technical Education

NYP **NANYANG**
THE INNOVATIVE POLYTECHNIC

NGEE ANN
POLYTECHNIC

**NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE**

NUS
National University
of Singapore

**REPUBLIC
POLYTECHNIC**
DISCOVER. TRANSFORM. ACHIEVE

SIT **SINGAPORE
INSTITUTE OF
TECHNOLOGY**

SP Singapore
Polytechnic

SMU
SINGAPORE MANAGEMENT
UNIVERSITY

SUTD
SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES

Temasek
POLYTECHNIC

Our Story...

We are an independent cybersecurity association that believes in developing, supporting as well as enhancing industry technical competence and management expertise to promote the integrity, status and interests of Information Security Professionals in Singapore.

We believe that through promoting the development, increase and spread of cybersecurity knowledge, and any related subject, we help shape more resilient economies.

Our Vision

A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem.

Our Mission

AiSP aims to be the pillar for Information Security Professionals and the overall Information Security Profession through:

- promoting the integrity, status and interests of Information Security Professionals in Singapore.
- enhancing technical competency and management expertise in cybersecurity.
- bolstering the development, increase and spread of information security knowledge and its related subjects.

AiSP Secretariat Team



Freddy Tan
Director



Vincent Toh
Associate Director



Elle Ng
Senior Executive



Karen Ong
Executive



www.AiSP.sg



secretariat@aisp.sg



+65 8878 5686 (Office Hours from 9am to 5pm)



6 Raffles Boulevard, JustCo, Marina Square, #03-308,
Singapore 039594

Please [email](#) us for any enquiries.